UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,981	07/16/2003	Roy M. Brooks	CIS03-25(7365)	8822

7590   10/16/2006

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

EXAMINER
OLATUNJI, OLATUNDE O

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>07/16/2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>07/16/2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Claim(s) 1-39 have been presented for examination.

Claim Objections

Claims 2, 6, 20 and 24 are objected to because of the following informalities:

Claims 2 and 6 both depends from claim 1 which states a "filter complex" while claim 2

and 6 both state a "filtering complex" this doesn't follow consistency with the claims.

Also claims 20 and 24 both depends from claim 19 that states a "filter complex" while

claims 20 and 24 state a "filtering complex" these claims are objected for the same

reason as above. Appropriate correction is required.

Claim 23 is objected to because of the following informalities: Claim 23 recites

the limitation "network management server and filter router device" in claim 23 that

depends on claim 12. There is insufficient antecedent basis for this limitation in the

claim. For the purpose of applying art claim 23 will be construed as being a dependent

of claim 22 which supply an antecedent basis for the network management server and

filter router.

Claim 34 is objected to because of the following informalities: Claim 34 recites

the limitation "routing processor, first transport mechanism, target node, filter router and

filter complex" in claim 34. There is insufficient antecedent basis for this limitation in the

claim. For the purpose of applying art claim 34 will be construed as being a dependent

of claim 19 which supply an antecedent basis for the routing processor, first transport

mechanism, target node, filter router and filter complex.

Claim 36 is objected to because of the following informalities: The claim states

the word "bifrucate" which appears to be a misspelling and would be construed as

bifurcate for the sake of prosecution. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

Claims 37 and 38 are rejected under 35 U.S.C. 101 because the claimed

invention is directed to non-statutory subject matter. Claim 37 is directed to a computer

readable medium. In this instance, this subject matter is not limited to that which falls

within a statutory category of invention because it is not limited to a process, machine,

manufacture, or a composition of matter. Instead, Applicant's specification provides

intrinsic evidence on page 18 line numbers 14-15, it includes the operations and

methods may be implemented in a software executable object or as a set of instructions

embedded in a carrier wave.

A set of instructions embedded in a carrier wave are not limited to media which

falls within a statutory category since they are clearly not a series of steps or acts to

constitute a process, not limited to a mechanical device or combination of mechanical

devices to constitute a machine, nor a tangible physical article or object which is some

form of matter to be a product and constitute a manufacture, nor a composition of two or

more substances to constitute a composition of matter.

Claim 38 as indicated in the preamble of the claim is directed towards a

computer data signal embodying program code, which is software per se, thus is not

statutory. Assuming that applicant meant for claim 38 to be a method claim, the

examiner notes that the method is not directed towards any practical application as no

concrete, useful, and tangible result is produced. In fact, as no steps are recited at all

for claim 38, no results of any sort are produced.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claims 2, 17, 19-35 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite.

For claim 2, a claim cannot depend upon it self and the broadest reasonable

understanding would be to construe claim 2 as being a dependent to claim 1.

The term "quantity sufficient" in claim 17 is a relative term, which renders the

claim indefinite. The term " quantity sufficient " is not defined by the claim, the

specification does not provide a standard for ascertaining the requisite degree, and one

of ordinary skill in the art would not be reasonably apprised of the scope of the

invention. Appropriate correction is required.

Claim 19, states the network management server comprises a network intrusion

detector monitor, a routing processor, and a filter complex. In the specification the

network management server states to include a network interface, a network monitor, a

routing processor and a routing table DB (see page 11, lines 25-27; Fig. 3, element 16).

The specification also state the network management server is in communication with

the filter complex (see page 6, line 1-2). This information renders the claim to be

inconsistent with the specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-12,14-30, 32-39 are rejected under 35 U.S.C. 102(b) as being

anticipated by Afek et al., US PG Pub. 2002/0083175 A1

With the respect to claims 1, 37, 38 and 39, Afek reference teaches receiving an

indication (see page 13, ¶ [0284]) of undesirable message traffic (see page 10, ¶ [0252],

"overload traffic") directed to a particular target node (page 10, ¶ [0252], victim

machines) via a first transport mechanism (see page 10, ¶ [0252], communication

channel) in a communications network (see page 10, ¶ [0245]);

rerouting all message traffic (see page 13, ¶ [0286], rerouting) carried via the first

transport mechanism (see page 10, ¶ [0252], communication channel) in the

communications network (see page 10, ¶ [0245]), and directed to the particular target

node (page 10, ¶ [0252], victim machines), to a filter complex (see page 9, ¶ [0242])

operable to distinguish desirable message traffic (see page 11, ¶ [0261], appropriate

message) from undesirable message traffic (see page 10, ¶ [0252], "overload traffic");

and

directing the filtering complex (see page 9, ¶ [0242]) to transmit, via a second

transport mechanism (see page 10, ¶ [0252], secure channel as SSH) over the

communications network (see page 10, ¶ [0245]), the desirable message traffic (see

page 11, ¶ [0261], appropriate message) to the target node (page 11, ¶ [0261], victim

machines).

With the respect to claims 2 and 20, Afek reference teaches a directing the

filtering complex to filter the message traffic (see page 10, ¶ [0253]) to subdivide

desirable message traffic (see page 11, ¶ [0261], appropriate message) from

undesirable message traffic (see page 10, ¶ [0252], "overload traffic"; page 13, ¶

[0288]).

With the respect to claims 3 and 21, Afek reference teaches wherein the filter

complex further comprises a security filter having filtering logic for performing filtering

(see page 13, ¶ [0293], rules), the security filter operable to parse the message traffic

and identify sequences in the message traffic indicative of undesirable message traffic

(see page 13, ¶ [0288] & [0295]).

With the respect to claims 4 and 22, Afek reference teaches a wherein the filter

complex further includes a filter routing device in communication with other routing

devices in the communications network (see page 14, ¶ [0301], "working in connection

with the routers") and coupled to the security filter for analyzing message traffic (see

page 13, ¶ [0293] & ¶ [0295]).

With the respect to claims 5 and 23, Afek reference teaches a wherein the filter routing device (see page 14, ¶ [0304]) in the filtering complex (see page 14, ¶ [0291], element 10) is operable to communicate according to the first transport mechanism (see page 10, ¶ [0252], communication channel) and the second transport mechanism (see page 10, ¶ [0252], secure channel as SSH).

With the respect to claims 6 and 24, Afek reference teaches wherein the rerouting all message traffic (see page 13, ¶ [0286], rerouting) includes directing the filter complex from a network management server in communication with the filter complex (see page 14, ¶ [0298]), the network management server operable to send a reroute message to the filtering complex (see page 14, ¶ [0298]).

With the respect to claims 7 and 25, Afek reference teaches directing a target node router serving the target node (page 11, ¶ [0261], victim machines) from the network management server (see page 10, ¶ [0252]), the network management server operable to send a redirect message to the target node router (see page 1, ¶ [0015]; page 14, ¶ [0298]).

With the respect to claims 8 and 26, Afek reference teaches the reroute message (see page 10, ¶ [0252]) is indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node (see page 8, ¶ [0214]) via the target node router serving the target node (see page 2, ¶ [0016], victim).

With the respect to claims 9 and 27, Afek reference teaches wherein the redirect message (see page 11, ¶ [0257], alert) is indicative that the target router serving the target node is not to receive message traffic (see page 11, ¶ [0257]) according to the

first transport mechanism corresponding to the target node (see page 11, ¶ [0257],

victim).

With the respect to claims 10 and 28, Afek reference teaches wherein the

redirect message is indicative that the target node router (see page 13, ¶ [0290])

serving the target node (see page 10, ¶ [0247], "potential victims") receives the

desirable message traffic in the second transport mechanism corresponding to the

target node.

With the respect to claim 11, Afek reference teaches wherein first and second

transport mechanisms coexist on a common physical network (see Figure 1, page 9, ¶

[0240]).

With the respect to claims 12 and 30, Afek reference teaches wherein first

transport mechanism corresponds to a public access protocol (see page 9, ¶ [0241], IP

network) adapted for communication via a plurality of dissimilar network switching

devices (see page 9, ¶ [0241], "switches").

With the respect to claims 14 and 32, Afek reference teaches wherein rerouting

all message traffic (see page 13, ¶ [0286], rerouting) further comprises propagating, via

a standard protocol (see page 9, ¶ [0241], Internet) corresponding to the first transport

mechanism, a node address other than the node address corresponding to the target

node.

With the respect to claims 15 and 33, Afek reference teaches wherein directing

the filter complex further comprises propagating routing information according to a

predetermined protocol (see page 2, ¶ [0016]), the routing information operable to

designate the target node (see page 2, ¶ [0016], victim) as the destination of the

message according to the second transport mechanism (see page 2, ¶ [0017]).

With the respect to claims 16 and 34, Afek reference teaches wherein rerouting

all message traffic is a static route (see page 2, ¶ [0016]; page 11, ¶ [0267]), according

to the first transport mechanism (see page 10, ¶ [0252], communication channel), from

a single router serving the target node (see abstract, "second set") to the filter router

(see page 14, ¶ [0304]) serving the filter complex (see fig. 2).

With the respect to claim 17, Afek reference teaches wherein receiving an

indication (see page 13, ¶ [0284]) further comprises detecting a pattern of undesirable

message traffic in quantity sufficient to be recognized (see page 3, ¶ [0039]).

With the respect to claims 18 and 35, Afek reference teaches wherein the

undesirable message traffic (see page 10, ¶ [0252], "overload traffic") emanates from a

plurality of sources (see page 1, ¶ [0002], DDOS), each of the plurality of sources

independently contributing substantially insignificant volume of message traffic (see

page 1, ¶ [0002], DDOS).

With the respect to claim 19, Afek reference teaches a network management

server (see page 10, ¶ [0252], "NOC (Network Operations Center)", "SNMP") for

redirecting undesirable message traffic (see page 10, ¶ [0252], "overload traffic")

comprising:

a network intrusion detector monitor operable to receive an indication (see page

10, ¶ [0252], sending authenticated messages, signal) of undesirable message traffic

(see page 10, ¶ [0252], "overload traffic") directed to a particular target node (page 10, ¶ [0252], victim machines) via a first transport mechanism (see page 10, ¶ [0252], communication channel) in a communications network;   .

a routing processor operable to propagate routing information to reroute all message traffic (see page 10, ¶ [0252], diverting routers) using the first transport mechanism (see page 10, ¶ [0252], communication channel) directed to the particular target node (page 10, ¶ [0252], victim machines); and

a filter complex responsive to the rerouting processor (see page 10, ¶ [0252], the guards), the filter complex operable to distinguish desirable message traffic from undesirable message traffic (see page 13, ¶ [0288]), and further operable to transmit, via a second transport mechanism (see page 10, ¶ [0252], secure channel as SSH) over the communications network, the desirable message traffic (see page 11, ¶ [0261], appropriate message) to the target node (page 11, ¶ [0261], victim machines).

With the respect to claim 29, wherein a network interface in the network management server is compatible with the first and second transport mechanisms (see page 16, ¶ [0319]) and wherein first and second transport mechanisms coexist on a common physical network (see Figure 1, page 9, ¶ [0240]).

With the respect to claim 36, Afek reference teaches in a network management server (see page 10, ¶ [0252], "NOC (Network Operations Center)", "SNMP") of a networked system of data communications devices, a method for transparently

intercepting, filtering, and rerouting message traffic for recovering from a distributed

denial of service attack comprising:

Detecting (see page 2, ¶ [0019]; page 13, ¶ [0282]), at a network monitor in the

network management server, a pattern of inundating undesirable message traffic (see

page 10, ¶ [0252], "overload traffic") to a particular target node (page 10, ¶ [0252],

victim machines) via a first transport mechanism (see page 10, ¶ [0252], communication

channel) in a communications network (see page 10, ¶ [0245]);

receiving, via a routing processor, an indication (see page 13, ¶ [0284]) of the

undesirable message traffic (see page 10, ¶ [0252], "overload traffic") directed to the

particular target node (page 10, ¶ [0252], victim machines);

transmitting, via a network interface, a reroute message (see page 1, ¶ [0011],

page 13, ¶ [0284]) to a filter complex (see page 13, ¶ [0284], guard machines) having a

security filter operable to distinguish desirable message traffic (see page 11, ¶ [0261],

appropriate message) from undesirable message traffic (see page 10, ¶ [0252],

"overload traffic"); and

rerouting, via a filter routing device in the filter complex, all message traffic (see

page 13, ¶ [0286]) carried via the first transport mechanism (see page 10, ¶ [0252],

communication channel) in the communications network (see page 10, ¶ [0245]) and

directed to the particular target node (see page 10, ¶ [0252], victim machines);

filtering, at the security filter, the message traffic to bifurcate (see page 13, ¶

[0293]) desirable message traffic (see page 11, ¶ [0261], appropriate message) from

undesirable message traffic (see page 10, ¶ [0252], "overload traffic");

transmitting, via the network interface to a target node router serving the target

node, a redirect message indicating that the target node router is to receive (see page

1, ¶ [0011]), via the second transport mechanism (see page 10, ¶ [0252], secure

channel as SSH), the desirable message traffic (see page 11, ¶ [0261], appropriate

message) directed to the particular target node and rerouted to the filter complex (see

page 13, ¶ [0293]), the filter complex and the target node router conversant in the first

transport mechanism (see page 10, ¶ [0252], communication channel) and the second

transport mechanism (see page 10, ¶ [0252], secure channel as SSH); and

directing, from the network management server, the filtering complex to transmit,

via a second transport mechanism (see page 10, ¶ [0252], secure channel as SSH)

over the communications network (see page 10, ¶ [0245]), the desirable message traffic

to the target node (see page 11, ¶ [0261]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 13 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Afek et al, U.S. PG Pub # 2002/0083175 as applied to claims above, and further in

view of Desai et al, U.S. PG Pub # 2003/0188189.

With the respect to claims 13 and 31, Afek reference teaches all the above. Afek

reference doesn't t teach wherein the second transport mechanism corresponds to a

virtual private network operable to encapsulate message packets of dissimilar protocols

such that the encapsulated message packets are recognized by a routing protocol of

the virtual private network. Desai reference teaches wherein the second transport

mechanism corresponds to a virtual private network (see page 1, ¶ [0012]; page 3, ¶

[0044], VPNs) operable to encapsulate message packets of dissimilar protocols such

that the encapsulated message packets are recognized by a routing protocol of the

virtual private network (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs). It would have

been obvious at the time the invention was made to a person having ordinary skill in the

art to which said subject matter pertains to have modified Afek reference which teaches

use of SSH (see Afek, page 10, ¶ [0252], "SSH") to include the use of Virtual private

network like in Desai reference for the purpose to ensure secure data transfer (see

Desai, page 3, ¶ [0044]).

Prior Art Made of Record

The prior art made of record and not relied upon in considered pertinent to

applicant's disclose. The following patents and patent applications are cited to further

show the state of the art with respect to methods and apparatus for network message

traffic redirection, such as:

United States Patent No. 6,704,873 to Underwood, is cited to show a secure

gateway interconnection in an E-Commerce base environment.

United States Patent No. 6,993,660 to Libenzi et al., is cited to show a system and method for performing efficient computer virus scanning of transient messages using checksums in a distributed computing environment.

United States PG Pub No. 2003/0204621 to Poletto et al., is cited to show architecture to thwart denial of service attacks.

United States PG Pub No. 2002/0133586 to Shanklin et al., is cited to show a method and device for monitoring data traffic and preventing unauthorized access to a network.

United States PG Pub No. 2004/0010712 to Hui et al., is cited to show an integrated VPN/Firewall System.

United States PG Pub No. 2003/0110379 to Ylonen et al., is cited to show an application gateway system, and method for maintaining security in a packet-switched information network.

Conclusion

All claims are rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Olatunde Olatunji whose telephone number is (571) 270-1020. The examiner can normally be reached on M-TR 7:30-5pm EST & 2nd Friday 7:30-4pm EST.
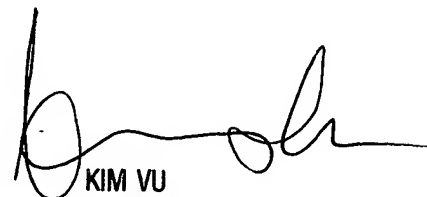
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

$O. O_n$
Olatunde Olatunji
10/4/2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100